NoPhish – Anti-Phishing Training

Research group SECUSO explains how to protect yourself

Phishing – What is it?

The term “Phishing“ refers to attempts to fool people into giving away their highly sensitive data by means of **fraudulent messages (via Emails, Skype or social networks)**. This data might be passwords, account information, creditcard details or malicious software (e.g. viruses). Phishers can easily send millions of phishing messages without great effort or expense, so even if only a small number of users fall for their scams it is still lucrative. These messages encourage recipients to click on malicious links. To prevent phishing attacks effectively, knowledge about the structure of web addresses (URLs) is fundamental. The following basic rules allow Internet users to detect phishing attacks effectively.

7 basic rules:

1. Check all links before clicking on them. Caution: The **actual URL** is not necessarily the same as the displayed URL. To examine the actual URL hover the mouse cursor over the displayed link (on mobile devices use your finger).

2. Pay full attention to the so called **who-section** when checking the URL. The who-section is simply the last two terms before the first stand-alone „/“ (in this case, facebook.com) of a URL.

   https://www. facebook.com /login/

   Who-Section

3. Do not enter any information if an **IP address** is provided:
   - ✗ https://95.130.22.98/google.com.secure-login.com

4. **Do not be fooled** by the following kinds of phishing URLs. This URL will take you to online-shopping, but the Phisher wants you to think you’re going to amazon.com:
   - ✗ https://www.amazon.com.bestonlineshops.com/
   - ✗ http://bestonlineshops.com/https://www.amazon.com

5. Carefully examine the who-section for **typos and inverted letters**:
   - ✗ https://www.reaaltorr.com/

6. Carefully examine the who-section for the use of **similar looking letters and numbers**:
   - ✗ https://www.instagrarn.com/

7. Carefully check whether the who-section is a **modification** of the known and trusted who-section. If you are unsure, use a search engine
   - ✗ https://www.facebook-secured.com/

Research group SECUSO

The research group SECUSO - Security - Usability - Society - of the Technische Universität Darmstadt contains people with backgrounds in computer science, psychology, social science, and communication science. Their goal is to develop security- and privacy-preserving mechanisms, which are both usable and protective. Awareness and educational approaches are also developed by this group.

Further information and the NoPhish app:
https://www.secuso.org/nophish

08/01/2017

SECUSO
SECURITY · USABILITY · SOCIETY

TECHNISCHE
UNIVERSITÄT
DARMSTADT